associates 17894 clifton park lane • cleveland, ohio 44107 • (216) 228-2045

January 10, 1994

Federal Communication Commission
2025 M Street
Washington, DC 20554

RE: Public Comment: Docket No. 93-292
Proposed Toll Fraud Rules

Gentlemen:

RAK Associates has been a telecommunication consulting firm for the past twenty-eight years. That experience, coupled with the fact that I am a recognized expert in the area of toll fraud, causes me to want to comment on the above FCC docket. These comments are based upon the fact that:

.... Over the past years I have served as the managing administrator for numerous telephone systems.

.... As of this date, no system which I have designed, installed and administered has been penetrated by a toll fraud attempt. Attempts have been made but so far they have fortunately been thwarted.

.... I have been involved in a number of fraud situations on other systems.

To begin with, the FCC position that the carrier tariffs are too restrictive placing the entire responsibility and liability for toll fraud on the telephone system owner is, in my view, correct. In my opinion, there is enough "blame" to be shared across the entire carrier, equipment vendor (both manufacturer and local distributor) and end user areas. Based on my experience, the following facts are true:

1. Toll fraud via CPE (Customer Premise Equipment) only became a major problem at the time responsibility for calling card fraud was transferred to the carrier through limitations imposed by the Truth In Lending Act. At that time, the carries were provided with an incentive to prevent that fraud. Their efforts materially reduced calling card fraud causing the CPE portion of the problem to balloon. This results in two conclusions:

   a. The reduction in calling card fraud indicates the carriers do have a method whereby they may control outgoing fraud in a proactive manner. Further, their present fraud control activity would further substantiate this capability.

   b. The carrier is the only organization having instant and continuing access to all of the outgoing and incoming traffic on their system.

2. The manufacturer continues to provide features which either facilitate the fraud or at least do little to protect a system. For example, the continued provision of Direct Inward System Access as a "standard" feature with little or no warning of the vulnerability this creates to the purchaser only perpetuates a common method of hacker access. But more importantly, the remote maintenance port provided on the telephone or voice mail system increasingly provides the hacker with a method of breaching system security while providing little or no protection. Protection can be provided through the use of the typical call-back modem providing maintenance port access to only specific pre-programmed telephone numbers. However, it has been my experience when requesting this as part of a system acquisition, that it is strongly resisted by both the manufacturer and/or the distributor. Their reasoning is that this would make remote maintenance more difficult.

3. The organization which installs and maintains the system may or may not be the manufacturer. However, in the vast majority of systems, it is these technicians on which the implementation of any protective measures are solely dependent. In fact, many of the penetrations by hackers, particularly as it relates to criminal activity, begin with information secured from the supplier's technicians. Yet it is these suppliers who specifically in their purchase agreements and renewal of maintenance contracts are inserting clauses eliminating any liability in the toll fraud area. Because of restrictions placed on support either by the manufacturer's certified technicians; denial of access to

maintenance port codes by the supplier; etc., it does not become simply a matter of changing maintenance support to avoid these onerous clauses.

4. Probably the most damaging fact at the customer level is the "it can't happen to me" attitude. Regardless of whether this is the fault of false bravado or the fact that the exposure is minimized or not even mentioned by the suppliers, the fact of the matter is that the customer is least likely to be able to protect themselves. The vast majority of telephone systems are installed in small businesses. It is unreasonable to expect that the administrators of those systems, who generally have multiple other duties, are going to be sufficiently knowledgeable in the area of communications to implement and monitor status for ongoing security.

To one degree or another, all of these parties (IXC carrier, local telephone company, manufacturer, installer and customer) have some level of responsibility to prevent or at least take those steps necessary to attempt to prevent toll fraud. With Docket 93-292, the Federal Communication Commission has the opportunity to take major steps to prevent fraud by placing protective requirements on the equipment and installation process itself. For example, the following requirements would provide a high level of protection:

1. The requirement for the installation of a call-back modem capability to protect the remote maintenance port.

2. The requirement that the direct inward system access feature only be provided as a separate purchase option.

3. A voice mail system should be designed with several levels of mandatory protection:

   a. The automatic elimination after a specified period of time of those voice mailboxes utilizing the default password.

   b. Software requiring the mandatory change of passwords after a specified period of time or the deletion of the mailbox.

   c. The ability to automatically turn-off the mailbox and notify the administrator of three successive failed attempts at a password.

The incorporation of these items in the CPE equipment and their activation will significantly reduce the exposure to hacker penetration. There are a number of possible software steps which can be taken in the system either at the discretion of the installation team or the direction of the customer. It is too easy to simply ignore these possibilities out of a desire to minimize the installation labor (those associated with a new system or software upgrade/changes) or out of ignorance. Requiring the customer to review a check list containing these items and the installation force to certify their implementation unless written deviation requested by the customer is provided would assure the implementation of that protection.

All of these steps should have the effect of reducing the potential exposure to the hacker or fraudulent telephone call. This would also clearly establish some level of liability on the part of the manufacturer not providing the requisite protection; the installer not implementing the requisite protection or the customer deliberately requesting that the protection not be implemented. In that regard, one additional step should be possible. Specifically, the customer should be able to request additional protection brought about by either new technology or further steps they may desire to take with the system provider only able to refuse to implement this protection with the assumption of the risk for any fraud which takes place.

Finally, history has proven that as fast as methods of blocking the fraudulent call are implemented, the perpetrators find new and more inventive ways to continue their fraudulent practices. Therefore, the line of final defense must eventually return to the carrier, both local and long distance. Experience with the fraud units of the inter-exchange carriers indicate an ability on their part to detect changes in calling patterns involving relatively small call quantities. At the present time, while this capability may exist, there is no responsibility associated with that capability. Therefore, it would be recommended that some "cap" be applied to liability on the customer's part in the absence of notification of possible fraud by the carrier. This liability limit would only be invoked in the event that:

1. The customer has invoked all of the potential protections.

2. In spite of incorporating these protective measures the fraud still occurs and the carrier does not notify the customer of the occurrence. Because many of these occurrences occur over weekends, the customer should either be given a choice of either providing a weekend contact or allowing the carrier to automatically disconnect long distance service if a notification is necessary.

I am sure that these are not all of the solutions. However, if something is to be done, it is necessary that some level of responsibility be placed upon the people and the organizations to implement protective steps (i.e., the manufacturers, the installation vendor and the carrier). I hope these thoughts will be taken into consideration in the Final Order. I appreciate the opportunity to provide these thoughts to the Federal Communication Commission and look forward to some relief from the toll fraud problem.

Cordially,

Richard A. Kuehn

RAK/bas